



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,743	12/06/2001	David W. Aucsmith	10559/463001/P10875	2946
20985	7590	06/09/2006		EXAMINER
FISH & RICHARDSON, PC P.O. BOX 1022 MINNEAPOLIS, MN 55440-1022			SANDOVAL, KRISTIN D	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 06/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/010,743	AUCSMITH ET AL.	
	Examiner Kristin Derwich	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 30 March 2006.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-22,28-35 and 39-52 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-22,28-35 and 39-52 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 06 December 2001 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 3, 11, 20, 23-27, 36-39, 43 and 44 are cancelled. Claims 1-22, 28-35, 39-46 and 47-52 are pending.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 30, 2006 has been entered.

2. Claim 40 rejected under 35 U.S.C. 102(e) as being anticipated by Lyle, U.S. Patent No. 6,886,102.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. Claims 1-2, 6-8, 9-10, 14-22, 28-34 and 41, 45, 46, 48 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack), U.S. Patent No. 6,298,445 in view of Lyle, U.S. Patent No. 6,886,102 and further in view of Shipley, U.S. Patent No. 6,119,236.

As per claim 1:

Shostack discloses a method comprising:

detecting possible security problems at client locations (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problems across a network in real time to a home location remotely located from the locations (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

determining at the home location an anomaly based on at least the possible security problems (7:15-16, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

transmitting notice of the anomaly in real time to the client locations (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach transmitting notice of the anomaly to the client location at which the possible security problem is detected. However, Lyle discloses a method wherein an event, which consists of an actual or suspected attack, is determined based on information gleaned from an internal source called a sniffer (6:52-7:18). Lyle also discloses a method wherein the responsive action, such as a message is sent to the device with the actual or suspected attack (8:21-59).

Shostack and Lyle fail to teach updating, in real time, firewalls protecting the client locations to account for the anomaly. However, Shipley discloses a method wherein a firewall is dynamically programmed, in real time, to allow for the firewall to change its response to various security breaches that occur (7:58-8:41).

As per claim 9, this is a computer readable medium version of the claimed method discussed above in claim 1 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 2:

Shostack further discloses a method further comprising transmitting notice of the anomaly in real time to other client locations that may communicate with the home location over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 10, this is a computer readable medium version of the claimed method discussed above in claim 2 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 6:

Shostack further discloses a method in which the anomaly includes unauthorized access to the network (4:64-67; 5:1, wherein this is an example of a security vulnerability (4:47-48) and the security vulnerabilities function as anomalies).

As per claim 14, this is a computer readable medium version of the claimed method discussed above in claim 6 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 7:

Shostack further discloses a method in which the anomaly includes unauthorized access of a resource accessible through the network (5:1-4, wherein the program library is a network resource).

As per claim 15, this is a computer readable medium version of the claimed method discussed above in claim 7 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 8:

Shostack further discloses a method in which the anomaly includes unauthorized use of resources available through the network (6:10-13, wherein seeing the disk is using a network resource).

As per claim 16, this is a computer readable medium version of the claimed method discussed above in claim 8 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claims 17 and 40:

Shostack discloses a method comprising:

At a home location in a network, receiving from at least two remote clients indications of possible security problems at the clients (6:66-67; 7:1, the first application is used to transmit notice of possible security problems and the second application functions to receive information from the first application.);

determining in real time at the home location an existence of an anomaly based on at least the indications of the possible security problems (7:20-27, wherein the security vulnerabilities function as anomalies).

Sending in real time, from a home location to a remote clients, information for updating security software to protect the remote clients to account for the anomaly (abstract, 2:31-3:37).

Shostack fails to teach receiving indications of possible security problems from at least two remote clients. However, Lyle discloses a method wherein messages of possible anomalies comes from a sniffer, which can scan one or more clients on the network, and a message from another domain that may contain anomalies (6:52-7:65).

Shostack and Lyle fail to teach the updates being applied to a firewall. However, Shipley discloses dynamically programming firewalls in real time to account for an anomaly (7:58-8:41).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with the invention of Shipley because each uses firewalls in their own inventions individually (Lyle, 6:37-51; Shostack, 4:13-21) and utilizing Shipley's real time dynamic programming of the firewalls would allow the firewalls to better protect their respective networks since it would constantly be modified to account for the newest threats (Shipley, 2:56-65).

As per claim 18:

Shostack further discloses a method further comprising transmitting notice of the existence of the anomaly in real time from the home location to the remote client locations (7:57-63, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

As per claim 19:

Shostack further discloses a method further comprising notice of the existence of transmitting the anomaly in real time from the home location to other remote client locations that may communicate with the home location over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 21:

Shostack further discloses a method of claim further comprising transmitting information from the home location to the remote client locations to help the remote client location identify possible security problems (13:7-9, wherein the database updates to the security vulnerabilities helps to identify possible security problems).

As per claim 22:

Shostack further discloses a method further comprising determining the existence of the anomaly based on at least information regarding previous anomalies (9:56-63, wherein the database contains a log of all of the previous security vulnerabilities which function as anomalies).

As per claim 29:

Lyle further discloses an apparatus in which the first mechanism also determines the anomaly based on at least information regarding previously determined anomalies (7:66-8:11).

As per claim 30:

Shostack discloses a system comprising:
a server (9:10);
for each of the client terminals,
a first client mechanism accessible by the client terminal to detect a possible security problem at the client terminal (6:43-46, wherein an intrusion is a possible security problem),
a second client mechanism accessible by the client terminal to transmit notice of the possible security problem across a network in real time to a server remotely located

from the client terminal (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem), and

a third client mechanism accessible by the client terminal to receive updates from the server in real time regarding security problems that the first client mechanism may use in detecting possible security problems (7:57-63; 9:10-21, wherein the client receives the software enhancement updates which function as updates from the server about security problems);

a first server mechanism accessible by the server to determine an anomaly based on at least information from a client regarding a possible security problems (7:15-16, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

a second server mechanism accessible by the server to transmit notice of the anomaly in real time over the network to the client terminals (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach receiving indications of possible security problems from at least two remote clients. However, Lyle discloses a method wherein messages of possible anomalies comes from a sniffer, which can scan one or more clients on the network, and a message from another domain that may contain anomalies (6:52-7:65). Lyle also discloses a method wherein the responsive action, such as a message is sent to the device with the actual or suspected attack (8:21-59).

Shostack and Lyle fail to teach the updates being applied to a firewall. However, Shipley discloses dynamically programming firewalls in real time to account for an anomaly (7:58-8:41).

As per claim 28 this is an apparatus version of the claimed system discussed above in claim 30 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 32:

Shostack further discloses a system in which the first server mechanism is also configured to determine the anomaly based on at least information regarding previously determined anomalies (9:56-63, wherein the database contains a log of all of the previous security vulnerabilities which function as anomalies).

As per claim 33:

Shostack further discloses a system in which the second server mechanism is also configured to transmit notice of the anomaly in real time to other client locations that may communicate with the server over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 34:

Shostack further discloses a system further comprising a firewall located between the client terminals and the server and configured to act as an intermediary for information flowing between the client terminals and the server (4:19-24, since the server is remotely connected to the network 20 (9:13-14; fig 2, item 20), the placement of the firewall makes it an intermediary between the external server and the client, therefore, the

firewall's functionality as a filter shows that information flows between the server and client).

As per claim 41:

Shostack discloses a method comprising:
detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);
transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);
transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly based on the possible security problem. However, Lyle discloses searching for a particular file type associated with a known intrusion technique (10:44-59).

Shostack and Lyle fail to teach determining an anomaly by searching for particular information in the anomaly. However, Shipley discloses a method wherein the type of information being searched for includes commands restricted to one type of user followed by commands restricted to another type of user all coming from the same sender address (6:4-30).

As per claims 45 and 48:

Shipley further discloses a method further comprising storing and performing complex analysis of anomaly trends by using a complexity theory mechanism (5:58-6:3).

As per claim 46:

Lyle further discloses a method wherein a wide view mechanism such as an analysis framework module, collects and maintains information regarding events reported to the server (7:50-65) which includes a statistics mechanism to compute and store records of events (8:12-20).

As per claims 47 and 49:

Lyle further discloses a method further comprising a statistics mechanism to compute and store records of anomalies (8:12-39).

As per claims 50 and 51:

Shipley further discloses a method further comprising updating, in real time, a firewall protecting the client location to account for the anomaly (7:58-8:41).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28), not only do vulnerabilities updates need to be disseminated, but tracking the hacker who breached the security is also essential in the security of a system against intrusions in order to ensure that the same person cannot do so again.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with the invention of Shipley because each uses firewalls in their own inventions individually (Lyle, 6:37-51; Shostack, 4:13-21) and utilizing Shipley's real time dynamic programming of the

Art Unit: 2132

firewalls would allow the firewalls to better protect their respective networks since it would constantly be modified to account for the newest threats (Shipley, 2:56-65).

4. Claims 4, 12 and 31 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) in view of Shipley (U.S. 6,119,236) as applied to claims 1, 9, 23, 26 and 30 above and further in view of Baker, U.S. Patent No. 6,775,657.

As per claim 4:

Shostack, Lyle and Shipley fail to teach a method further comprising inspecting a packet that arrives at the client location to detect the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

As per claim 12, this is a computer readable medium version of the claimed method discussed above in claim 4 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 31:

Shostack, Lyle and Shipley fail to teach a system in which the first mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem. However, Baker discloses a method wherein a network based intrusion

detection system analyzes network packet data to make security decisions (1:41-42; 46-53).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28), not only do vulnerabilities updates need to be disseminated, but tracking the hacker who breached the security is also essential in the security of a system against intrusions in order to ensure that the same person cannot do so again.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with the invention of Shipley because each uses firewalls in their own inventions individually (Lyle, 6:37-51; Shostack, 4:13-21) and utilizing Shipley's real time dynamic programming of the firewalls would allow the firewalls to better protect their respective networks since it would constantly be modified to account for the newest threats (Shipley, 2:56-65).

5. Claims 5, 13 and 35 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) as applied to claims 1, 9 and 30 above and further in view of Bowman-Amuah, U.S. Patent No. 6,697,824.

As per claim 5:

Shostack and Lyle fail to teach a method in which the network includes a virtual private network. However, Bowman-Amuah discloses a method wherein a network is protected from unauthorized access through the encryption services provided by Virtual Private Networking (75:64-65, fig 36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a virtual private network with the network because of the added security benefits a VPN affords a system against unauthorized users.

As per claim 13, this is a computer readable medium version of the claimed method discussed above in claim 5 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 35:

Shostack and Lyle fail to teach a system in which at least one of the firewalls includes a corporate server. However, Bowman-Amuah discloses a method wherein a corporate firewall includes a corporate server at a corporate headquarters (75:65-66; 76:19-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a corporate server with the firewall because if the intrusion detection system were to be used in a business setting the firewalls would provide increased access control for the internal network (76:21-23).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28), not only do vulnerabilities updates need to be disseminated, but tracking the hacker who breached the

security is also essential in the security of a system against intrusions in order to ensure that the same person cannot do so again.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with the invention of Shipley because each uses firewalls in their own inventions individually (Lyle, 6:37-51; Shostack, 4:13-21) and utilizing Shipley's real time dynamic programming of the firewalls would allow the firewalls to better protect their respective networks since it would constantly be modified to account for the newest threats (Shipley, 2:56-65).

6. Claims 42 and 52 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) and further in view of Moran, U.S. Patent No. 6,826,697.

As per claim 42:

Shostack discloses a method comprising:
detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);
transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location, including searching for an unexpected login. However, Lyle discloses a method wherein the event, which consists of an attack, is compared to other events that have occurred (7:50-8:11).

Shostack and Lyle fail to teach a method in which determining the anomaly comprises searching for an unexpected login. However, Moran discloses a method wherein failed login attempts are logged (19:41-20:18). A failed login attempt is an unexpected login since it is not a correct login. The login is not expecting for the login information to be wrong, therefore a failed login qualifies as an unexpected login by an unexpected user.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with Moran because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28), the ability to detect further types of attacks such as forward and backward time steps in a log file or an overflow buffer attack as stated in Moran (4:1-37) would increase the security against attacks as a whole.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

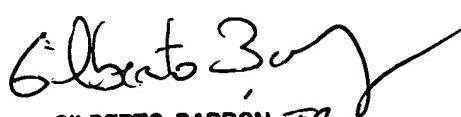
Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kristin Derwich
Examiner
Art Unit 2132


KMD


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100